

**ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ
в «Московский Нефтехимический банк» публичном акционерном обществе**

1. Общие положения

Настоящее Положение об обработке персональных данных клиентов (далее – Положение) устанавливает порядок и условия проведения работ по обработке персональных данных (далее - ПДн) клиентов – представителей юридических лиц и физических лиц (далее - клиенты) «Московский Нефтехимический банк» публичного акционерного общества (далее - Банк) с использованием средств автоматизации и без использования таких средств.

Положение разработано с целью обеспечения защиты прав и свобод субъекта персональных данных (далее - субъект ПДн) при обработке его ПДн, а также с целью установления ответственности должностных лиц Банка, имеющих доступ к ПДн его клиентов, за невыполнение требований и норм, регулирующих обработку ПДн.

Данное Положение разработано в соответствии с требованиями:

- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";
- Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 19 августа 2011 года № 706 «Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных»;
- Письмо Банка России от 14.03.2014 г. № 42-Т «Об усилении контроля за рисками, возникающими у кредитной организации при использовании информации содержащей персональные данные граждан».
- Методических рекомендаций по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации и пр.

Настоящее Положение вступает в силу с момента его утверждения Правлением Банка и действует бессрочно до замены его новым Положением или до наступления иных случаев, предусмотренных законодательством.

Настоящее Положение является обязательным для исполнения всеми сотрудниками Банка, имеющими доступ к ПДн клиентов – субъектов ПДн. Все сотрудники Банка, связанные с обработкой ПДн и имеющих доступ к ПДн клиентов, должны быть ознакомлены с настоящим Положением под роспись.

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля (надзора), а также в целях закрепления наработанной Банком практики операций с ПДн.

Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм настоящего Положения возлагается на Председателя комитета по информационной безопасности.

При появлении новых типов ПДн допускается разграничение доступа к ним на основании приказа Председателя Правления .

Банк учитывает требования настоящего Положения при разработке и утверждении любых внутренних документов Банка, связанных с обработкой ПДн.

2. Основные понятия и определения

В Положении применяются термины и определения в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», «Положении об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденном Постановлением Правительства РФ от 17 ноября 2007 г. № 781, «Положении об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденном Постановлением Правительства РФ от 15 сентября 2008 года № 687, другими нормативно-правовыми актами, регуливающими защиту прав субъектов ПДн и обеспечение безопасности ПДн.

3. Состав ПДн

ПДн клиентов Банка – это любая информация, относящаяся к прямо или косвенно определенному или определяемому клиенту Банка (субъекту ПДн) - физическому лицу. Перечень ПДн, обрабатываемых в Банке (далее – Перечень ПДн), приведен в Приложении 1. В ходе осуществления Банком своих функций Перечень ПДн может быть изменен. При получении ПДн, не указанных в Перечне ПДн, указанные данные подлежат немедленному уничтожению лицом, непреднамеренно получившим указанные данные.

4. Специальные категории ПДн

Запрещается обрабатывать ПДн о политических, религиозных и философских убеждениях, а также об интимной жизни клиента Банка. Указанные специальные категории ПДн в деятельности Банка не используются и не обрабатываются.

Банк не вправе производить обработку данных о судимости клиента, за исключением в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Данные о здоровье обрабатываются Банком только в том случае, если эти данные прямо относятся к возможности клиента исполнять свои обязательства перед Банком, либо используются в целях исполнения требований действующего законодательства, например, в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

Сведения о расовой и национальной принадлежности клиентов Банком не обрабатываются. Фотографии, находящиеся в документах, удостоверяющего личность клиента Банка, и иные аналогичные данные не относятся к сведениям о расовой и национальной принадлежности.

В случае если обработка специальных категорий ПДн клиента Банка необходима по действующему законодательству или для осуществления деятельности Банка, то такая обработка осуществляется с письменного согласия клиента, за исключением случаев, предусмотренных законодательством Российской Федерации в области ПДн.

5. Биометрические ПДн

Банк не обрабатывает сведения, которые характеризуют физиологические особенности клиентов и на основе которых можно установить их личность. В соответствии с требованиями ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Данные изображения лица» система охранного видеонаблюдения, используемая в Банке, не обрабатывает биометрические ПДн, на основании которых возможно идентифицировать личность клиента Банка.

Сканирование фотографий в документах, идентифицирующих личность клиентов (например, в паспортах), в Банке не осуществляется. Передаваемые в рамках договоров с определенными третьими копии паспортов клиентов не соответствуют требованиям, предъявляемым к форматам записи изображения, установленными ГОСТ Р ИСО/МЭК 19794-5-2006.

В случае если обработка биометрических ПДн клиента Банка необходима по действующему законодательству или для осуществления деятельности Банка, то такая обработка осуществляется с письменного согласия клиента, за исключением случаев, предусмотренных законодательством Российской Федерации в области ПДн.

6. Общедоступные ПДн

В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн с письменного согласия клиента могут включаться его фамилия, имя, отчество, год и место рождения, адрес, включая адрес электронной почты, клиентский номер, IP-адрес, сведения о профессии и иные ПДн, сообщаемые субъектом ПДн или находящиеся в Перечне ПДн.

Сведения о клиенте Банка должны быть в любое время исключены из общедоступных источников ПДн по запросу клиента либо по решению суда или иных уполномоченных государственных органов.

В случае обработки общедоступных ПДн клиента обязанность доказывания того, что обрабатываемые ПДн являются общедоступными, возлагается на Банк.

7. Цели и сроки обработки ПДн

Банк обрабатывает ПДн с целью осуществления возложенных на Банк законодательством Российской Федерации функций в соответствии с (в том числе, но не ограничиваясь) », Гражданским кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности, «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О персональных данных», «О бухгалтерском учете», принятыми в их исполнение нормативными актами Правительства России, а также в соответствии с нормативными актами Банка России и в иных целях в рамках действующего законодательства. Банк собирает ПДн только в объеме, необходимом для достижения названных целей.

Допускаются иные цели обработки ПДн в случае, если указанные действия не противоречат действующему законодательству, деятельности Банка и на проведение указанной обработки получено согласие клиента Банка.

Хранение ПДн осуществляется в соответствии с согласием субъектов ПДн и в течение срока, указанного в согласии с учетом требований законодательства.

В случае отсутствия в указанных нормативно-правовых актах сроков хранения отдельных видов ПДн, указанные ПДн подлежат хранению в течение срока, указанного в согласии соответствующего субъекта ПДн.

8. Обработка ПДн

Банк осуществляет обработку ПДн в целях соблюдения законодательных и нормативных актов, минимизации банковских рисков (включая сохранность активов и ресурсов Банка), зависящих от ПДн клиента.

Обработку ПДн осуществляют сотрудники Банка, уполномоченные на то должностными инструкциями, иными внутренними документами Банка или организационно-распорядительными документами по Банку.

Сотрудники Банка имеют право получать только те ПДн, которые необходимы им для выполнения конкретных должностных обязанностей.

Сотрудники Банка, осуществляющие обработку ПДн клиентов, должны быть проинформированы о факте такой обработки, об особенностях и правилах такой обработки, установленных нормативно-правовыми актами и внутренними документами Банка.

В рамках информирования сотрудников Банка о факте обработки ПДн, Банк обязывает сотрудников Банка самостоятельно изучать и соблюдать внутренние нормативные документы, регламентирующие как общий порядок работы с ПДн, так и специальные нормы, касающиеся совершения отдельных действий, связанных с обработкой ПДн клиентов Банка.

9. Согласие на обработку ПДн

Обработка ПДн клиентов осуществляется с их согласия на обработку их ПДн, а также в иных случаях, предусмотренных статьей 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Согласие на обработку ПДн может быть дано клиентом или его законным представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя клиента полномочия данного представителя проверяются Банком. Форма согласия может быть в письменной, конклюдентной или иной форме, предусмотренной действующим законодательством. При недееспособности клиента письменное согласие на обработку его данных дает его законный представитель.

Банк обязан иметь доказательство получения согласия клиента на обработку его ПДн (в том случае, если такое согласие является необходимым).

9.1. Письменная форма согласия

В случаях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта персональных данных:

Обработка специальных категорий ПДн,

Обработка биометрических ПДн,

Трансграничная передача ПДн в страны, не обеспечивающие адекватной защиты прав субъекта ПДн,

Включение в общедоступные источники ПДн,

Принятие решений на основании исключительно автоматизированной обработки ПДн.

Согласие клиента на обработку его ПДн в Банке должно включать в себя сведения и информацию, требующуюся для включения в согласие в соответствии с действующим законодательством и внутренними документами Банка.

9.2. Конклюдентная форма согласия

В соответствии со статьей 158 Гражданского кодекса Российской Федерации конклюдентное или подразумеваемое согласие – это действия лица, выражающие его волю установить правоотношение (например, совершить сделку), но не в форме устного или письменного волеизъявления, а поведением, по которому можно сделать заключение о таком намерении.

Клиенты Банка дают конклюдентное согласие на обработку их ПДн в случаях, описанных в Таблица 1.

Таблица 1. Случаи обработки ПДн на основании конклюдентного согласия

Вид обработки ПДн	Цель обработки	Обрабатываемые ПДн
Заполнение анкет, в т.ч. и на Web-сайте Банка.	Изучение возможностей по получению и обслуживанию кредита.	п.2.1.3 Перечня ПДн
Предоставление удостоверения личности для прохода на территорию Банка.	Проход на территорию Банка.	Фамилия, имя, отчество, а также паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.
Регистрация на Web-сайте и мероприятиях, проводимых Банком	Уведомление о мероприятиях, акциях, предоставляемых скидках	Фамилия, имя, отчество, контактная информация.
Участие в опросах, проводимых Банком.	Проведение опросов и исследований в области финансовых услуг, проведения маркетинговых программ, статистических исследований.	п.2.1.3 Перечня ПДн.

9.3. Отзыв согласия

Клиент Банка может в любой момент отозвать свое согласие на обработку ПДн при условии, что подобная процедура не нарушает требований законодательства РФ и допускается условиями договора, одной из сторон по которому является Банк, а клиент является либо другой стороной по договору, либо выгодоприобретателем, либо поручителем.

В случае отзыва клиентом Банка согласия на обработку ПДн Банк вправе продолжить обработку ПДн без согласия клиента при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9.4. Обработка ПДн без согласия

В соответствии с пунктами 2 - 11 части 1 статьи 6, а также пунктом 4 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» обработка ПДн может осуществляться без согласия. В Банке к таким ситуациям относятся те, которые указаны в Таблице 2.

Таблица 2.

Случаи обработки ПДн без согласия (по состоянию законодательства на дату утверждения Положения)

Вид обработки ПДн	Основание
Заключение договора с клиентом	Ст.6.1.5 ФЗ-152
Взаимодействие с Пенсионным фондом РФ	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с налоговыми органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с налоговыми органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с таможенными органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Федеральной службой финансового мониторинга	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Банком России	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами предварительного следствия	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами внутренних дел	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами внутренних дел	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с судебными органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с судебными органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие со Счетной палатой Российской Федерации	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Фондом социального страхования Российской Федерации	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами принудительного исполнения судебных актов, актов других органов и должностных лиц	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с организациями, осуществляющими функции по обязательному страхованию вкладов	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с лицами, указанными клиентом Банка в завещательном распоряжении	Ст.6.1.1 ФЗ-152, ст.26 ФЗ ФЗ- 395-1 и ст.1128 ГК РФ
Взаимодействие с нотариальными конторами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с иностранными консульскими учреждениями	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Заполнение анкет и заявок на получение кредитов	Ст.6.1.5 ФЗ-152
Оформление договоров аренды, лизинга, доверительного управления, в которых клиент Банка указан как выгодоприобретатель	Ст.6.1.5 ФЗ-152
Заполнение анкет и заявок на получение кредитов	Ст.6.1.5 ФЗ-152
Оформление договоров аренды, лизинга, доверительного управления, в которых клиент Банка указан как выгодоприобретатель	Ст.6.1.5 ФЗ-152
Идентификация клиентов в рамках законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма	Ст.6.1.1 ФЗ-152 и ФЗ-115
Расчет платежными поручениями	Ст.6.1.1 ФЗ-152 и ст.863 ГК РФ, а также Положения Банка России 383-П

Открытие вклада в пользу третьего лица	Ст.6.1.1 ФЗ-152 и ст.842 ГК РФ, а также Положения Банка России 2-П и 222-П
Распоряжение денежными средствами по требованиям третьих лиц	Ст.6.1.1 ФЗ-152 и ст.847 ГК РФ, а также Положения Банка России 2-П и 222-П
Обработка доверенностей	Ст.6.1.1 ФЗ-152, ст.185 ГК РФ и ФЗ-115
Обработка ПДн представителей дилеров (юридических лиц)	Ст.6.1.1 ФЗ-152 и ст.182 ГК РФ
Взаимодействие с организациями по взысканию задолженностей (в порядке и на условиях, предусмотренных законодательством)	Ст.6.1.1 ФЗ-152, ст.382 – 390 ГК РФ

10. Порядок обработки ПДн с использованием средств автоматизации

Обработка ПДн в Банке может проводиться с использованием средств автоматизации (информационных систем) и без таковых. Конкретный способ обработки ПДн определяется на основании процедур использования данных, определенных внутренними документами Банка.

Обработка ПДн в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативных и методических документов ФСТЭК и ФСБ России по защите информации, а также Комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

Банк осуществляет обработку ПДн в ИСПДн структурных подразделений Банка. К ИСПДн Банка отнесены информационные системы, поддерживающие выполнение возложенных на Банк законодательством РФ функций, в которых обрабатываются ПДн, содержащиеся в Перечне ПДн.

Список информационных систем, в которых обрабатываются ПДн, их классификация, требования по обеспечению безопасности обрабатываемых в них ПДн клиентов Банка описаны в отдельных нормативных документах Банка.

Контроль за соответствием обработки ПДн заявленным целям возлагается на лицо, ответственное за обработку ПДн в Банке, и на руководителей соответствующих подразделений.

Необходимость доступа работников Банка к ПДн, обрабатываемым в ИСПДн Банка, документально определена в их должностных инструкциях

10.1. Исключительно автоматизированная обработка ПДн

Исключительно автоматизированная обработка ПДн в Банке не осуществляется. Во всех процессах обработки ПДн клиентов с использованием средств автоматизации принимают участие ответственные сотрудники Банка.

10.2. Порядок обработки ПДн без использования средств автоматизации

Обработка ПДн без использования средств автоматизации (далее – неавтоматизированная обработка ПДн) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

При неавтоматизированной обработке ПДн на бумажных носителях:

- не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы;
- ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие ПДн, формируются в дела в зависимости от цели обработки ПДн;
- дела с документами, содержащими ПДн, должны иметь внутренние описи документов с указанием цели обработки и категории ПДн.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес оператора и лиц, которым оператором поручена обработка ПДн, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;
- типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, - при необходимости получения письменного согласия на обработку ПДн;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

Неавтоматизированная обработка ПДн в электронном виде осуществляется на внешних электронных носителях информации. При отсутствии технологической возможности осуществления неавтоматизированной обработки ПДн в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка соответствующих средств защиты информации), исключающие возможность несанкционированного доступа к ПДн лиц, не допущенных к их обработке.

Электронные носители информации, содержащие ПДн, учитываются в журнале учета электронных носителей ПДн. К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории ПДн.

При несовместимости целей неавтоматизированной обработки ПДн, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Документы и внешние электронные носители информации, содержащие ПДн, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

11. Получение/сбор ПДн

Источниками ПДн клиентов в Банке являются:

Анкеты,

Резюме,

Договоры,

Формы,

Сайт Банка,

Заявки/заявления,

Информация с рецепции,

Телефон,

Копии предоставляемых документов,

иные источники в соответствии с действующим законодательством Российской Федерации.

Клиент обязан предоставлять Банку достоверные сведения о себе и своевременно сообщать Банку об изменении своих ПДн. Банк имеет право проверять достоверность сведений, предоставленных субъектом, сверяя данные, предоставленные субъектом, с имеющимися у Банка документами.

12. Получение ПДн не напрямую от клиента Банка

Банк получает ПДн клиента от него самого или от третьих лиц при условии наличия согласия на обработку и/или оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». В ряде случаев Банк получает персональные данные от третьих лиц, получающих ПДн у субъектов, в том числе в качестве представителей Банка на основании доверенности, а также имеющих договорные отношения с субъектом ПДн либо с Банком. В качестве таких третьих лиц могут выступать: банки-партнеры, страховые организации-партнеры и другие лица. В данном случае, в соответствии с частью 4 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Банк не обязан получать согласие субъекта ПДн на обработку его ПДн. Если ПДн получены не от субъекта ПДн и их обработка не поручена Банку оператором, Банк до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» права субъекта ПДн;
- источник получения ПДн.

Банк освобождается от обязанности предоставить субъекту ПДн указанные сведения в случаях, если:

- ПДн получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является клиент Банка.
- ПДн сделаны общедоступными клиентом Банка или получены из общедоступного источника.

Банк осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы клиента Банка.

Предоставление клиенту Банка сведений, предусмотренных ч. 3 ст. 18 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», нарушает права и законные интересы третьих лиц.

13. Использование ПДн

Доступ к ПДн субъекта имеют сотрудники Банка, которым ПДн необходимы в связи с исполнением ими трудовых обязанностей. Перечень сотрудников, имеющих доступ к ПДн, утверждается приказом Председателя Правления по Банку.

Доступ сотрудников, не включенных в вышеуказанный перечень, осуществляется на основании приказа Председателя Правления, подготовленного на основании служебной записки руководителя сотрудника с положительной резолюцией ответственного за обработку ПДн в Банке. В случае если Банку оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к ПДн клиентов Банка, то соответствующие данные предоставляются Банком только после подписания с лицами, осуществляющими обработку ПДн по поручению Банка, соответствующего соглашения, в котором должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Использование и хранение биометрических и специальных категорий ПДн вне информационных систем ПДн может осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих

данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

14. Использование ПДн с целью идентификации клиентов

В ходе выполнения функций кредитной организации, связанных с необходимостью идентификации состоящих на обслуживании клиентов, Банк в соответствии с Федеральным законом №115-ФЗ от 07.08.2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем» обязан обрабатывать следующие персональные данные клиентов:

- фамилия, имя, отчество;
- полная дата и место рождения;
- паспортные данные;
- место жительства, прописки.
- гражданство,
- идентификационный номер налогоплательщика (если имеется).
- номера контактных телефонов и факсов (если имеются).

Письменное согласие на обработку указанной информации от субъекта ПДн не требуется на основании пункта 3 части 1 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» в силу того, что обработка осуществляется в соответствии с Федеральным законом №115-ФЗ от 07.08.2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем».

15. Использование ПДн с целью выдачи кредитов

В ходе выполнения функций кредитной организации, связанных с проведением операций по выдаче и погашению гарантий, кредитов и займов (включая учет векселей и иных документарных ценных бумаг), Банк также обрабатывает ПДн клиента, указанные в Приложении 1 к настоящему Положению. Среди них в том числе:

- образование, данные об ученых степенях;
- финансовое положение (доходы, долги, владение имуществом, денежные вклады, полученные гарантии и субсидии и др.);
- факты биографии и трудовая деятельность (место работы, размер заработка, судимость, служба в вооруженных силах, работа на выборных должностях, на государственной службе, участие в профессиональных объединениях и профсоюзах и др.).

В случае если указанные данные предоставлены на этапе рассмотрения заявки на предоставление кредита, и кредитный договор не был заключен, то их обработка завершается, а данные уничтожаются в течение 4 (четырёх) лет от даты их предоставления. В случае же если кредитный либо иной подобный договор был заключен, обработка ПДн завершается в течение срока, указанного в согласии на обработку.

Согласие на обработку указанных ПДн получается у потенциального заемщика до заключения кредитного договора и начала обработки таких данных.

16. Использование ПДн субъекта в целях продвижения товаров, работ, услуг

Клиент Банка дает свое согласие на обработку его ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с клиентом Банка с помощью средств связи, включая, но, не ограничиваясь: почтовая рассылка, рассылка SMS-сообщений, электронная почта, телефон (включая мобильный), факсимильная связь, сеть Интернет, только при следующих условиях:

- Действие данного согласия распространяется только на
- проведение опросов и исследований в области финансовых услуг,
- проведение маркетинговых программ,
- проведение статистических исследований,
- уведомления о мероприятиях, акциях, предоставляемых скидках.

Действие данного согласия распространяется только на взаимоотношения, возникающие в рамках исполнения Банком обязательств по заключенным с клиентом договорам.

Действие данного согласия распространяется на следующие операции по обработке ПДн: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Данное согласие действует в течение срока, указанного в таком согласии.

В остальных случаях обработка ПДн в целях продвижения работ и услуг на рынке путем прямых контактов с клиентом Банка с помощью средств связи допускается только с его предварительного согласия. Бремя доказывания наличия согласия лежит на Банке. Банк обязан немедленно прекратить по требованию клиента обработку его ПДн, если это не противоречит действующему законодательству.

17. Передача ПДн третьим лицам

Передача ПДн третьим лицам (включая надзорные органы) возможна только в случаях, прямо предусмотренных законодательными и нормативными актами, либо в случае согласия субъекта ПДн.

В случае если обязанность либо возможность предоставления имеющихся в распоряжении Банка ПДн иным лицам (включая органы государственной и муниципальной власти) установлена законодательством, Банк обязан предоставить указанные данные в составе, виде и сроки, указанные в законодательных или нормативных актах.

Если обязанность предоставления ПДн фиксируется соответствующим запросом (ходатайством) уполномоченного лица, запрос подлежит обязательной проверке в целях контроля над обоснованностью предоставления запроса. При обоснованности подобного запроса, юридический отдел информирует об этом подразделение, которое осуществляет обработку запрошенных данных, которое в свою очередь формирует ответ на запрос (при необходимости – организует деятельность иных подразделений по подготовке ответа). При необоснованности запроса, юридический отдел информирует об этом подразделение, которое осуществляет обработку запрошенных данных, которое в свою очередь направляет отправителю запроса письменное уведомление об отказе в предоставлении ПДн.

Любые запросы на раскрытие ПДн от третьих лиц, не являющихся субъектами раскрываемых ПДн, подлежат обязательному рассмотрению на предмет обоснованности.

При передаче ПДн третьим лицам Банк обязан уведомлять лиц, получивших ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие ПДн, обязаны соблюдать их конфиденциальность и безопасность. Данное требование не распространяется на обмен ПДн в порядке, установленном законодательством.

Третьи лица и цели передачи им ПДн клиентов ФБР указаны в Таблица 3, а также в разделе «Передача ПДн третьим лицам без согласия».

Таблица 3. Перечень третьих лиц, которым возможна передача ПДн клиента

Тип третьего лица	Цель передачи
Бюро кредитных историй	Формирование, обработка и хранение кредитных историй клиентов, а также предоставление кредитных отчетов о клиентах
Организации по взысканию задолженностей	В случаях досудебного и судебного разбирательства при просрочке возврата кредита или его части.
Центры обработки вызовов	Для приема звонков Клиентов Банка и их переадресации уполномоченным сотрудникам Банка.
Страховые организации-партнеры	Предоставление страховых услуг и оформление документов в связи с услугами по страхованию

Передача ПДн третьим лицам осуществляется только с согласия клиента за исключением случаев, предусмотренных действующим законодательством.

18. Передача ПДн третьим лицам без согласия

В соответствии с Федеральным законом от 2 декабря 1990 г. N 395-1 «О банках и банковской деятельности» Банк вправе осуществлять передачу ПДн в соответствующих целях запроса объемах без согласия субъекта ПДн следующим третьим лицам:

- Пенсионный фонд РФ,
- Налоговые органы,
- Таможенные органы,
- Федеральную службу финансового мониторинга,
- Банк России,
- Органы предварительного следствия (при наличии согласия руководителя следственного органа),
- Органы внутренних дел,
- Судебные органы,
- Счетную палату Российской Федерации,
- Федеральный орган исполнительной власти в области финансовых рынков,
- Фонд социального страхования Российской Федерации,
- Органы принудительного исполнения судебных актов, актов других органов и должностных лиц в случаях, предусмотренных законодательными актами об их деятельности,
- Организации, осуществляющей функции по обязательному страхованию вкладов,
- Нотариальным конторам (по находящимся в их производстве наследственным делам о вкладах умерших клиентов),
- Иностранным консульским учреждениям (в отношении счетов иностранных граждан в случае смерти таких граждан),
- а также другим третьим лицам в случаях, предусмотренных законодательными актами об их деятельности.

19. Трансграничная передача ПДн

Трансграничная передача ПДн осуществляется Банком при осуществлении расчетной деятельности в порядке направления разъяснений в рамках исполнения требований национального законодательства о противодействии отмыванию доходов, полученных преступным путем и финансировании терроризма, персональных данных, обеспечивающей адекватную защиту прав субъектов ПДн.

Иная трансграничная передача осуществляется исключительно с письменного согласия субъекта ПДн.

20. Передача ПДн в государственные органы

В соответствии с действующим законодательством Банк вправе осуществлять передачу ПДн государственным органам, указанным в разделе «Передача ПДн третьим лицам без согласия», а также другим государственным органам и должностным лицам в случаях, предусмотренных законодательными актами об их деятельности.

21. Уточнение ПДн

Уточнение ПДн Клиента производится путем обновления или изменения данных в информационной системе или на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн клиента.

Уточнение ПДн производится в рамках действующей в Банке системы документооборота с соблюдением принципов, изложенных в настоящем Положении.

22. Блокирование ПДн

Блокирование ПДн представляет собой деятельность Банка по временному прекращению обработки ПДн Клиентов (за исключением случаев, если обработка необходима для уточнения ПДн). Блокирование осуществляется в случае, если клиентом Банка или его законным представителем, либо уполномоченным органом по защите прав субъектов ПДн выявлена недостоверность ПДн при условии, что такое блокирование не нарушает права и законные интересы клиента или третьих лиц.

23. Хранение ПДн

Хранение ПДн клиентов должно осуществляться в форме, позволяющей определить клиента, не дольше, чем этого требуют цели и сроки обработки ПДн, указанные в разделе «Цели и сроки обработки персональных данных» данного Положения. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Хранение ПДн клиентов, цели обработки которых различны, должно осуществляться раздельно в рамках информационной системы или, при условии хранения на материальных носителях, в рамках структуры дел соответствующего подразделения Банка. Сотрудник Банка, имеющий доступ к ПДн клиентов в связи с исполнением трудовых обязанностей - обеспечивает хранение информации, содержащей ПДн клиента, исключаящее доступ к ним третьих лиц.

В отсутствие сотрудника на его рабочем месте не должно находиться документов, содержащих ПДн клиентов.

При уходе в отпуск, служебную командировку и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие ПДн клиентов лицу, на которое локальным актом Банка будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, то документы и иные носители, содержащие ПДн клиентов, передаются другому сотруднику, имеющему доступ к ПДн клиентов по указанию руководителя структурного подразделения.

При увольнении сотрудника, имеющего доступ к ПДн клиентов, документы и иные носители, содержащие ПДн клиентов, передаются другому сотруднику, имеющему доступ к ПДн клиентов по указанию руководителя структурного подразделения и с уведомлением лица, ответственного за обработку ПДн в Банке.

24. Архивирование ПДн

ПДн, неиспользуемые в операционной деятельности Банка и цель обработки которых не достигнута, могут быть переведены на архивное хранение с соблюдением всех необходимых требований, предусмотренных Федеральным законом от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации» и иными нормативными актами в сфере организации хранения, комплектования, учета и использования архивных документов независимо от их форм собственности.

Архивирование ПДн производится в рамках действующих в Банке систем документооборота и работы с архивными документами с соблюдением принципов, изложенных в настоящем Положении. Обязательным условием архивирования ПДн является обеспечение их конфиденциальности и безопасности.

Подразделения Банка, хранящие архивные ПДн на бумажных носителях, обязаны обеспечить ограничение доступа к указанным данным только тех сотрудников, деятельность которых непосредственно связана с обработкой хранимого типа архивных ПДн. Доступ к архивным ПДн, хранение которых осуществляется на электронных носителях, должен быть ограничен исходя из требований информационной безопасности, указанных в данном Положении и отдельных локальных нормативных актах Банка.

25. Обезличивание ПДн

С целью уменьшения объема ПДн, подлежащих защите в соответствии с требованиями 152-ФЗ, подзаконных актов и методических указаний, а также в целях снижения нагрузки и

обременений на Банк, приводящих к дополнительным затратам без повышения уровня защищенности ПДн и прав клиентов Банка, может быть произведено обезличивание ПДн клиентов Банка. Также обезличивание производится в целях предоставления статистической отчетности, агрегированной информации о деятельности Банка, а также в иных целях, предусмотренных действующим законодательством, например, по достижении целей их обработки или в случае утраты необходимости в достижении этих целей в соответствии со статьей 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Обезличенные ПДн должны представлять собой информацию на бумажном или магнитном носителе, принадлежность которой к конкретному физическому лицу невозможно определить без использования дополнительной информации в силу произведенных при обработке ПДн действий. Применяемые в Банке механизмы обезличивания приведены в Таблица 4.

Таблица 4. Механизмы обезличивания ПДн

Алгоритм обезличивания	Описание	Примечание
Абстрагирование ПДн	Сделать ПДн менее точными путем группирования общих или непрерывных характеристик, т.е. не позволяющими отличить с помощью данного атрибута одного субъекта ПДн от других	Например, вместо указания конкретного возраста использовать кодификаторы (18-25 лет – 2, 26-33 года – 3 и т.д.).
Скрытие ПДн	Удалить всю или часть записи ПДн, не требуемые для деятельности организации БС РФ	Применяется в том случае, если Банк уже хранит неиспользуемые ПДн.
Внесение шума в ПДн	Добавить небольшое количество посторонней информации в ПДн	
Замена ПДн		Переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи
Замена данных средним значением		Заменить выбранные данные средним значением для группы ПДн
Разделение ПДн на части	Использование таблиц перекрестных ссылок	Например, вместо одной таблицы использовать две – одна с ФИО и идентификатором субъекта ПДн, вторая – с тем же идентификатором субъекта ПДн и остальной частью ПДн
Использование специальных алгоритмов	Маскирование ПДн или подмена определенных символов другими	Отдельные корпоративные СУБД могут быть оснащены специальными функциями маскирования (data masking pack).
Использование алгоритмов криптографического преобразования	Хэширование или шифрование	Использование средств криптографической защиты регулируется отдельным законодательством

Лицо, ответственное за обработку ПДн клиентов обладает правом самостоятельного обезличивания ПДн клиентов. При необходимости получения иных обезличенных ПДн, сотрудники Банка обязаны направить соответствующему лицу, ответственному за обработку ПДн

клиентов, служебную записку с запросом соответствующих данных, если предоставление таких данных не осуществляется в рамках должностных обязанностей и внутрибанковских регламентов.

26. Уничтожение ПДн

Уничтожение ПДн производится Банком:

- при выявлении неустранимых неправомерных действий с ПДн клиентов;
- по достижении целей обработки ПДн (при условии невозможности обезличивания ПДн);
- при получении от клиента отзыва согласия на обработку ПДн (при условии, что такой отзыв не противоречит обязанностям Банка продолжать обработку ПДн в соответствии с действующим законодательством);
- по требованию клиента или уполномоченного органа по защите прав субъектов ПДн – если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Уничтожению подлежат все требуемые к уничтожению ПДн, зафиксированные на материальных носителях или хранящихся в информационных системах. Уничтожение ПДн на материальных носителях производится в соответствии со стандартными внутрибанковскими процедурами. Уничтожение ПДн в информационных системах производится должностным лицом, использовавшим указанные данные. Ответственный за обработку ПДн Банка контролирует полноту уничтожения указанных данных в информационных системах Банка.

Если обработка ПДн осуществляется другим лицом, действующим по поручению Банка, то Банк обязан обеспечить их уничтожение в соответствии с данным Положением.

Решение об уничтожении ПДн принимается лицом, ответственным за обработку ПДн в Банке, по представлению руководителя подразделения, ответственного за обработку соответствующих ПДн клиентов, признанных необходимыми к уничтожению. Решение об уничтожении должно быть принято в срок, не превышающий 3 (трех) рабочих дней с даты появления оснований к уничтожению ПДн.

После принятия решения об уничтожении руководитель подразделения, ответственного за обработку ПДн, обязан уведомить об этом ответственного за обработку ПДн Банка, который назначает комиссию по уничтожению ПДн.

Данная комиссия получает (для данных, хранящихся на материальных носителях) полную информацию обо всех местах хранения соответствующих ПДн. Если хранение осуществлялось на материальном носителе, то руководитель соответствующего подразделения обязан передать комиссии указанный материальный носитель ПДн, подлежащих уничтожению.

Уничтожение ПДн производится руководителем подразделения (для данных, хранящихся в электронной форме) либо комиссией Банка по уничтожению ПДн (для документов на материальных носителях) в срок

не превышающий 10 (десяти) рабочих дней с даты выявления неустранимых неправомерных действий с ПДн.

не превышающий 30 (тридцати) календарных дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» или другими федеральными законами.

Не превышающий 30 (тридцати) календарных дней с даты поступления от клиента отзыва согласия на обработку его ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» или другими федеральными законами.

В случае отсутствия возможности уничтожения ПДн в течение срока, указанного выше, Банк осуществляет уничтожение или обеспечивает уничтожение ПДн в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

В случае если согласно имеющейся у Банка информации, ПДн клиентов были направлены третьим лицам, руководитель подразделения, осуществляющего обработку соответствующих ПДн, обязан потребовать у указанных третьих лиц в письменной форме уничтожения ПДн с изложением оснований для подобного уничтожения.

При необходимости уничтожения ПДн, являющихся частью материального носителя, содержащего ПДн, не подлежащие уничтожению, комиссией осуществляется вымарывание либо иное физическое удаление данных с условием сохранения данных, не подлежащих уничтожению. Скорректированный подобным образом документ подлежит возврату в соответствующее подразделение.

После уничтожения данных председатель комиссии обязан уведомить о данной операции подразделение, передавшее информацию на уничтожение.

При получении информации об уничтожении либо после самостоятельного уничтожения, подразделение, осуществлявшее обработку ПДн, обязано уведомить о факте уничтожения клиента и, в случае если уничтожение произведено по запросу уполномоченного органа по защите персональной информации, указанный орган.

Уведомление должно содержать перечень мер, предпринятых Банком по результатам обнаружения случаев неправомерной обработки ПДн.

Ответственный за обработку ПДн в Банке в рамках проверок по направлениям деятельности контролирует своевременность и полноту уничтожения ПДн руководителями подразделений.

27. Права и обязанности клиента Банка

В целях обеспечения защиты ПДн клиенту Банка в праве:

- получать полную информацию о своих ПДн и способе обработки этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом «О персональных данных». Физический доступ клиентов Банка на территорию Банка осуществляется в соответствии с внутренними документами Банка;
- требовать внесения необходимых изменений, уничтожения или блокирования соответствующих ПДн, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц Банка.

Субъект ПДн вправе обратиться в Банк с составленным с соблюдением требования законодательства запросом об обработке ПДн Банком. Запрос должен быть зарегистрирован и обработан в соответствии с Регламентом реагирования на запросы субъектов ПДн. В данном запросе может быть уточнена следующая информация:

- 1) подтверждение факта обработки ПДн Банком;
- 2) правовые основания и цели обработки ПДн;
- 3) цели и применяемые Банком способы обработки ПДн;
- 4) наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Банком или на основании федерального закона;
- 5) обрабатываемые ПДн, относящиеся к соответствующему Клиенту, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки ПДн, в том числе сроки их хранения;
- 7) порядок осуществления клиентом прав, предусмотренных федеральным законом;
- 8) информация об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные федеральным законодательством.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма или если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

Сведения, указанные выше, предоставляются клиенту или его представителю оператором при обращении либо при получении запроса клиента или его уполномоченного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность клиента или

его уполномоченного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие клиента в отношениях с Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Банком, подпись клиента или его уполномоченного представителя.

В случае, если сведения, указанные выше, а также обрабатываемые ПДн были предоставлены для ознакомления клиенту по его запросу, клиент вправе обратиться повторно к Банку или направить ему повторный запрос в целях получения сведений, указанных выше, и ознакомления с такими ПДн не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является клиент.

Клиент вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных выше, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в предыдущем абзаце, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

28. Права и обязанности Банка в отношении обработки ПДн

Необходимость доступа служащих Банка к ПДн субъектов ПДн, обрабатываемым в Банке, документально определена в соответствующих должностных инструкциях.

Обработка и защита ПДн в структурных подразделениях Банка осуществляется в документально определенном порядке, исключающем несанкционированный доступ к ПДн.

В Банке документально определен перечень лиц, осуществляющих обработку ПДн. Лица, осуществляющие такую обработку, проинформированы о факте обработки ими ПДн, об особенностях и правилах осуществления такой обработки, а также об ответственности за нарушение действующего законодательства в области ПДн. Лица, осуществляющие обработку ПДн, ознакомлены под роспись с настоящими требованиями и подписали обязательство о соблюдении конфиденциальности ПДн и соблюдении правил обработки ПДн.

В Банке документально определен перечень помещений, в которых ведется обработка ПДн, а также перечень лиц, имеющих допуск в помещения, в которых проводится обработка ПДн. Передача ПДн между структурными подразделениями Банка осуществляется только между сотрудниками, имеющими доступ к ПДн.

Банк не вправе заставлять клиентов к предоставлению ПДн, однако вправе требовать этого, если подобные обязательства прямо вытекают из договорных отношений с клиентами или требований нормативных и законодательных актов.

Банк обязан обеспечивать субъекту ПДн возможность ознакомления в доступной форме с документами и материалами, непосредственно к нему относящимися (если подобный запрет прямо не установлен действующим законодательством) при получении запроса, соответствующего требованиям статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и раздела «Права и обязанности клиентов Банка» данного Положения. Если сбор ПДн осуществляется во исполнение требований федерального закона, сотрудники Банка, осуществляющие сбор ПДн обязаны разъяснить субъекту ПДн юридические последствия отказа предоставить ПДн.

Банк обязан сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение 30 (тридцати) календарных дней с даты получения такого запроса.

29. Уведомление уполномоченного органа по защите прав субъектов ПДн

В случаях, установленных Федеральным законом «О персональных данных», Банк направляет уведомление в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор).

30. Обеспечение безопасности ПДн

Банк при обработке ПДн клиентов принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или

случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. Указанные меры, включая их перечень и описание, а также порядок их принятия установлены в Положении об обеспечении безопасности ПДн.

Обеспечение безопасности ПДн в Банке достигается, в частности:

- 1) определением угроз безопасности ПДн при их обработке в информационных системах ПДн;
- 2) применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- 4) оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;
- 5) учетом машинных носителей ПДн;
- 6) обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- 7) восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) установлением правил доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в информационной системе ПДн;
- 9) контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн.

Банк не должен обеспечивать безопасность и конфиденциальность ПДн клиентов в следующих случаях:

- ПДн обезличены;
- ПДн являются общедоступными или включены в источники общедоступных данных.

31. Ответственность за нарушение требований настоящего Положения

Сотрудники Банка, обрабатывающие ПДн Клиентов, и лица, которым Банк поручает обработку ПДн клиентов, несут гражданскую, уголовную, административную и иную предусмотренную законодательством Российской Федерации ответственность за нарушение режима защиты, обработки и порядка использования этих ПДн.

За неисполнение или ненадлежащее исполнение уполномоченными сотрудниками Банка по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с ПДн Банк вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

Административная ответственность также предусмотрена в случаях неправомерного отказа уполномоченными лицами Банка в предоставлении собранных в установленном порядке документов, в случаях несвоевременного предоставления таких документов, либо в случаях предоставления неполной или заведомо ложной информации.

Руководитель подразделения, предоставляющий доступ сотруднику Банка к обрабатываемым ПДн, несет персональную ответственность за данное разрешение.

Сотрудники Банка, получающие доступ к обрабатываемым ПДн, несут персональную ответственность за конфиденциальность полученной информации

Приложение 1
к Положению об обработке персональных данных клиентов
в «Московский Нефтехимический банк» публичное акционерное общество

Перечень ПДн клиентов

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Перечень (далее – Перечень») ПДн клиентов, подлежащих защите в Открытом акционерном обществе «Московский Нефтехимический банк» (далее – Банк), разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и внутренними документами Банка (далее - Банк).

2. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

2.1. В Банке сведениями, составляющими персональные данные (далее – ПДн) клиента, является любая информация, относящаяся к прямо или косвенно определенному или определяемому клиенту Банка (субъекту ПДн) - физическому лицу, в том числе:

2.1.1. ПДн специальной (первой) категории.

2.1.1.1. Сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья клиентов Банка.

2.1.2. Биометрические ПДн (второй категории).

2.1.2.1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Банком для установления личности клиента Банка. К числу таких данных *могут* относиться среди прочего видеозаписи внутренних систем охранного телевидения и банковских терминальных устройств, данные в устройствах, использующих для идентификации биометрические данные человека, ксерокопии с документов, удостоверяющих личность и имеющих фотографию владельца – клиента Банка. Обязательным условием отнесения указанных данных к разряду биометрических ПДн является условие их использование Банком для установления личности человека.

2.1.3. ПДн общей (третьей) категории

(за исключением ПДн, относящихся к специальной категории и к обезличенным, общедоступным, биометрическим ПДн).

2.1.3.1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.3.2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

2.1.3.3. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

2.1.3.4. Номера телефонов (мобильного и домашнего), в случае их регистрации на клиента Банка или по адресу его места жительства (по паспорту).

2.1.3.5. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения).

2.1.3.6. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение

2.1.3.7. Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях).

2.1.3.8. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

2.1.3.9. Содержание и реквизиты гражданско-правового договора с клиентом Банка, в котором он является стороной по договору, выгодоприобретателем или поручителем.

2.1.3.10. Сведения о заработной плате.

2.1.3.11. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет).

2.1.3.12. Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым

обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев).

2.1.3.13. Сведения об имуществе (имущественном положении):

- автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств);

- недвижимое имущество (полные адреса размещения объектов недвижимости);

- банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов);

- кредиты (займы), банковские счета (в том числе спецкартсчета), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, спецкартсчетов, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости).

2.1.3.14. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

2.1.3.15. Сведения об идентификационном номере налогоплательщика.

2.1.3.16. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

2.1.4. Общедоступные ПДн (четвертой категории).

2.1.4.1 Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.4.2. Номера телефонов (мобильного и домашнего), в случае их регистрации на клиента Банка или по адресу его места жительства (по паспорту).

2.1.4.3. IP-адреса устройств, с которых клиент Банка осуществляет доступ к информационным системам Банка.

2.1.4.4. Номер клиента или иной уникальный идентификатор клиента.

2.1.4.5. иные сведения, являющиеся общедоступными или сделанные таковыми с письменного согласия клиента.